

5

We claim:

1. In a network, a method comprising the steps of:

- 10 providing a web page with a first and second embedded software facility, said first embedded software facility including a reference to a source of computer-executable code for determining the trust proxy setting in a web browser, said second embedded software facility including a reference to a source of computer-executable code;
- 15 receiving a request for said web page from a web browser; and forwarding said web page to said web browser in response to said request.

2. The method of claim 1 wherein said computer-executable code referenced by said first embedded software facility is stored at a remote location from said web page.

- 20 3. The method of claim 1 wherein said computer-executable code referenced by said second embedded software facility is stored at a remote location from said web page.

4. In a network, a method comprising the steps of:

- 25 providing a web browser, said web browser stored on an electronic client device interfaced with said network, said web browser including settings for network connections;
- 30 retrieving a web page with said web browser, said web page including a first and second software facility stored therein, said first software facility including a reference to a source of computer-executable code for determining the trust proxy setting in said web browser;
- retrieving the code for said first software facility; and determining the trust proxy setting in the network settings of said web browser by executing the code for said first software facility.

- 35 5. The method of claim 4 wherein said the execution of the code referenced by said first software facility causes the trust proxy setting of said browser to be displayed to a user

- 5 of said electronic client device as part of a notification that said trust proxy setting is not enabled.
6. The method of claim 4 wherein said second software facility stored on said web page is a Java applet composed of multiple classes.
- 10 7. The method of claim 4 wherein said second software facility stored on said web page is a .jar file.
8. The method of claim 4 wherein both said first and second software facilities are Java applets.
- 15 9. The method of claim 4 wherein said computer-executable code referenced by said first embedded software facility is stored at a remote location from said web page.
- 20 10. The method of claim 4 wherein said computer-executable code referenced by said second embedded software facility is stored at a remote location from said web page.
11. In a network, a method for executing applets, said method comprising the steps of:
providing a web browser, said web browser stored on an electronic client device
25 interfaced with said network, said web browser including settings for network connections;
providing a first applet and second applet stored on a web page accessible over said network, said first applet including a reference to a source of computer-executable code for determining the trust proxy setting in said web browser;
30 retrieving said web page with said web browser, said web browser initiating execution of said first applet; and
determining the trust proxy setting in the network settings of said web browser as a result of the execution of said first applet.
- 35 12. The method of claim 11 wherein said first applet displays said trust proxy setting to a user of said web browser as part of a notification that said trust proxy setting is not enabled.

5

13. The method of claim 11 wherein said applets are Java applets.

14. The method of claim 11 said second applet is composed of multiple classes.

10 15. The method of claim 11 wherein said second applet is a compressed file.

16. The method of claim 11 wherein the code for said first applet is stored at a remote location from said web page.

15 17. In a computer network, a first and second medium holding computer-executable instructions for a method, said method comprising the steps of:
providing a web page with a first and second embedded software facility, said first embedded software facility including a reference to code stored in said first medium, said first medium holding computer-executable code for determining the trust proxy setting in a web browser, said second embedded software facility including a reference to code stored in said second medium;
20 receiving a request for said web page from a web browser; and forwarding in response to said request said web page.

25 18. The first medium of claim 17, wherein said first medium is located remotely from said web page storage location.

19. The second medium of claim 17 wherein said second medium is located remotely from said web page storage location.

30

20. The mediums of claim 17 wherein both said first medium and said second medium are located remotely from said web page.

21. In a network, a method comprising the steps of:

35 providing a first web page with a first embedded software facility, said first embedded software facility including a reference to a source of computer-executable code for determining the trust proxy setting in a web browser;

- 5 providing a second web page with a second embedded software facility, said second embedded software facility including a reference to a source of computer-executable code;
- receiving a first request for said first web page from a web browser;
- forwarding said first web page to said web browser in response to said first
- 10 request;
- receiving a second request for said second web page from said web browser after the execution of said first embedded software facility, said execution indicating the proxy setting in said web browser is enabled; and
- forwarding said second web page to said web browser in response to said second
- 15 request;
22. The method of claim 21 wherein said computer-executable code referenced by said first embedded software facility is stored at a remote location from said first web page.
- 20 23. The method of claim 21 wherein said computer-executable code referenced by said second embedded software facility is stored at a remote location from said second web page.